ABSTRACT OF THE DISCLOSURE

A communication network includes a Security Gatekeeper that authenticates and validates network control messages within, transiting, entering and leaving an overlying control fabric such as an SS7 network. The Security Gatekeeper incorporates several levels of checks to ensure that messages are properly authenticated, valid, and consistent with call progress and system status. In addition to message format, message content is checked to ensure that the originating node has the proper authority to send the message and to invoke the related functions and that the message, itself, is appropriately coded. Predefined sets of templates may be used to check the messages, each set of templates being associated with respective originating point codes and/or calling party addresses. The templates may also be associated with various system states such that messages corresponding to a particular template cause a state transition along a particular edge to a next state node for which another set of templates is defined. Thus, system, call and/or transaction state are maintained. The monitor also includes signaling point authentication using digital signatures and timestamps. Timestamps are also used to initiate appropriate timeouts and so that old or improperly sequenced message may be ignored, corrected or otherwise processed appropriately. The Security Gatekeeper may be located at the edge of a network to be protected so that all messaging to and from the protected network must enter and egress by way of the Gatekeeper. Alternatively, the Security Gatekeeper may be internal to the protected network. In this configuration, ISUP traffic can be monitored by configuring the Security Gatekeeper as a "pseudo switch" so that ISUP messaging is routed through the Gatekeeper on its way between interconnected SSPs, while actual bearer traffic is trunked directly between the associated SSPs, bypassing the Gatekeeper.